CLAIMS

What is claimed is:

1 A method for dispensing and evidencing indicia by an indicia generating device in a system having a plurality of indicia generating devices that have been divided into n groups, each of the indicia generating devices for generating and printing indicia on a media that is to be received at a plurality of establishments, wherein the establishments are associated with different geographic designations, the method comprising the steps of:

(a) receiving a plurality of verification keys, wherein each one of the received verification keys is encrypted as a function of a respective geographic designation;

(b) receiving a plurality of key IDs, wherein each one of the key IDs is associated with one of the verification keys and is encrypted as a function of the same geographic designation used to encrypt the corresponding verification key;

(c) in response to receiving a request to generate an indicium for a media destined for a particular one of the establishments, evidencing the indicium by;

(i) generating one of the verification keys and the corresponding key ID assigned to indicia generating device's group based on the geographic designation associated with the particular establishment, and

(ii) using the generated verification key to create a digital signature, and digitally signing the indicia by including the digital signature and the generated key ID in the indicia.

2 The method of claim 1 further including the steps of:

receiving a master secret key and a secret key; and

and generating the verification keys and the key IDs assigned to the group using the master secret key and a secret key.

3 The method of claim 2 further including the step of generating and printing indicia for postage on a mail piece that is to be received at a plurality of distribution centers.

4 The method of claim 4 further including the step of verifying the indicia at a destination distribution center.

5 The method of claim 4 further including the step of verifying the indicia at an originating distribution center.

6 The method of claim 3 further including the step of using zip codes to represent the geographic designations.

7 The method of claim 1 further including the step of generating and printing indicia for tickets.

8 The method of claim 1 further including the step of distributing to each one of the establishments, the verification keys and the key ID's that were encrypted as a function of the geographic designation associated with the establishment.

9 The method of claim 8 further including the step of verifying the indicia upon receipt at the particular establishment by using the key ID on the indicia and the distributed verifications keys to compute a digital signature, and comparing the computed digital signature with the digital signature on the indicia.

10 A computer readable media containing program instructions for dispensing and evidencing indicia by an indicia generating device in a system having a plurality of indicia generating devices that have been divided into n groups, each of the indicia generating devices for generating and printing indicia on a media that is to be received at a plurality of establishments, wherein the establishments are associated with different geographic designations, the instructions for:

(a) receiving a plurality of verification keys, wherein each one of the received verification keys is encrypted as a function of a respective geographic designation;

(b) receiving a plurality of key IDs, wherein each one of the key IDs is associated with on of the verification keys and is encrypted as a function of the same geographic designation used to encrypt the corresponding verification key;

(c) in response to receiving a request to generate an indicium for a media destined for a particular one of the establishments, evidencing the indicium by;

(i) generating one of the verification keys and the corresponding key ID assigned to indicia generating device's group based on the geographic designation associated with the particular establishment, and

(ii) using the generated verification key to create a digital signature, and digitally signing the indicia by including the digital signature and the generated key ID in the indicia.

11 The computer readable media of claim 10 further including the instructions of:

receiving a master secret key and a secret key; and

and generating the verification keys and the key IDs assigned to the group using the master secret key and a secret key.

12 The computer readable media of claim 11 further including the instruction of generating and printing indicia for postage on a mail piece that is to be received at a plurality of distribution centers.

13 The computer readable media of claim 12 further including the instruction of verifying the indicia at a destination distribution center.

14 The computer readable media of claim 12 further including the instruction of verifying

the indicia at an originating distribution center.

15 The computer readable media of claim 11 further including the instruction of using zip codes to represent the geographic designations.

16 The computer readable media of claim 10 further including the instruction of generating and printing indicia for tickets.

17 The computer readable media of claim 10 further including the instruction of distributing to each one of the establishments, the verification keys and the key ID's that were encrypted as a function of the geographic designation associated with the establishment.

18 The computer readable media of claim 17 further including the instruction of verifying the indicia upon receipt at the particular establishment by using the key ID on the indicia and the distributed verifications keys to compute a digital signature, and comparing the computed digital signature with the digital signature on the indicia.

19 An indicium generating device for generating and printing indicia on a media that is to be received at a plurality of establishments, wherein the establishments are associated with different geographic designations, comprising:

means for receiving a plurality of verification keys, wherein each one of the received verification keys is encrypted as a function of a respective geographic designation;

means for receiving a plurality of key IDs, wherein each one of the key IDs is associated with one of the verification keys and is encrypted as a function of the same geographic designation used to encrypt the corresponding verification key;

means for generating and evidencing an indicium for a media destined for a particular one of the establishments, including means for generating one of the verification keys and the corresponding key ID assigned to indicia generating device's group based on the geographic designation associated with the particular establishment, and means for creating a digital signature using the generated verification key and for digitally signing the indicia by including the digital signature and the generated key ID in the indicia.

20 The indicium generating device of claim 19 wherein the indicium generating device further receives a master secret key and a secret key, and generates the verification keys and the key IDs using the master secret key and a secret key.

21 The indicium generating device of claim 20 wherein the indicium is generated and printed as postage on a mail piece that is to be received at a plurality of distribution centers.

22 The indicium generating device of claim 21 wherein indicia is verified at a destination distribution center.

23 The indicium generating device of claim 21 wherein indicia is verified at an originating distribution center.

24 The indicium generating device of claim 20 wherein the geographic designations

comprise zip codes.

25 The indicium generating device of claim 19 wherein the indicium is generated and printed for tickets.

26 The indicium generating device of claim 19 wherein the verification keys and the key ID's that were encrypted as a function of the geographic designation associated with the establishment are distributed to each one of the establishments.

27 The indicium generating device of claim 26 wherein the indicia is verified upon receipt at the particular establishment by using the key ID on the indicia and the distributed verifications keys to compute a digital signature, and comparing the computed digital signature with the digital signature on the indicia.

28 A method for dispensing and evidencing postage indicia by a postage generating device (PGD) in a system having a plurality of PGDs that have been divided into n groups identified by a group designation G_i, $i = 1,\ldots$n, the method comprising the steps of:

(a) receiving a master secret key K and a secret key K_i;

(b) in response to receiving a request to generate an indicium for a mail piece destined for a particular postal destination *Dest*, generating the indicium;

(c) computing a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination;

(d) computing a key ID I_i^{Dest} as a function of the master secret key K and the postal destination;

(e) using the computed verification key V_i^{Dest} to create a digital signature for the indicia; and

(f) digitally signing the indicia by including the digital signature and the computed key ID I_i^{Dest} on the indicia.

29 The method of claim 28 further including the step of computing each verification key V_i^{Dest} as a one-way function H of the PGD group key K_i and a designation of the postal destination:

$$V_i^{Dest} = H(K_i, Dest).$$

30 The method of claim 29 further including the step of using ZIP codes to designate the postal destination.

31 The method of claim 30 further including the step of computing each of the key ID's as a one-way function H of the PGD group, G_i, the master secret key, K, and a designation of the postal destination, $Dest$:

$$I_i^{Dest} = H(K, Dest, G_i).$$